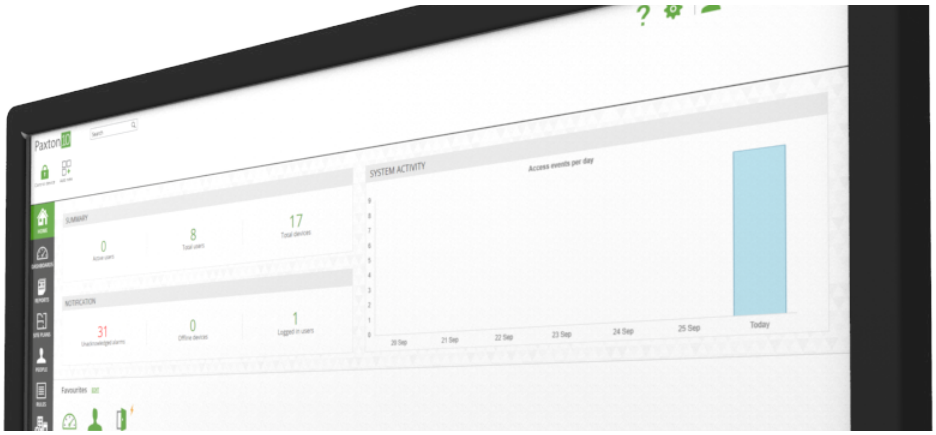

# Så använder man knappsatser med Paxton10

## Översikt

Knappsatsläsare kan utgöra ett utmärkt sätt att förbättra säkerheten och gardera mot användning av borttappade eller stulna autentiseringsuppgifter- och metoder. Knappsatsläsare kan lägga till ytterligare driftslägen för läsare i åtkomstpunkter eller styrbara enheter.

| Läsarens driftsläge | Användaråtgärd krävs | Användare identifierad |
|---|---|---|
| Endast passerbricka | Uppvisa en giltig passerbricka. | J |
| Endast PIN | Ange användarens PIN i knappsatsen. | J |
| Endast kod | Ange en av enheternas koder i knappsatsen. | N |
| Passerbricka + PIN | Uppvisa en giltig passerbricka. Ange sedan användarens PIN. Innehavaren av passerbrickan och PIN-koden måste tillhöra en och samma användare. | J |
| Passerbricka + kod | Uppvisa en giltig passerbricka. Ange därefter någon av enhetens koder. | J |
| Passerbricka eller PIN | Uppvisa en giltig passerbricka ELLER ange användarens PIN. | J |
| Passerbricka eller kod | Uppvisa en giltig passerbricka ELLER ange en av enhetens koder. | J/N |
| Passerbricka eller PIN eller kod | Uppvisa en giltig passerbricka ELLER ange användarens PIN ELLER ange en av enhetens koder. | J/N |

En kod tillhör en viss enhet medan en PIN tillhör en viss användare

# När man använder en Paxton10-knappsats

En knappsatsläsare från Paxton10 kan installeras istället för befintliga Paxton10-läsare.

## Säkerhet

Knappsatsläsare kan användas för att lägga till en till autentiseringsnivå genom att kräva sekundär bekräftelse från användare med passerbricka.

När detta används i driftsläget "**Passerbricka + PIN**" eller "**Passerbricka + kod**" kan inte obehöriga komma åt byggnaden enbart med en borttappad passerbricka eller kod, utan de behöver både en giltig passerbricka och tillhörande PIN eller dörrkod.

## Bekvämlighet

Det händer ofta att använder glömmer att ta med sig sina passerbrickor eller att de lämnar dem vid skrivbordet, vilket leder till att man blir utlåst. Genom att använda driftsläget "**Passerbricka eller PIN**" eller "Passerbricka eller kod" kan användare få åtkomst utan sin passerbricka, vilket är idealiskt för dörrar med låg säkerhetsnivå.

# Behörigheter

När en PIN eller passerbricka används ges åtkomstbehörighet av användarens byggnadsbehörigheter. Om endast kod används är inte användaren inte känd - då ges åtkomst förutsatt att koden är giltig för enheten i fråga.

# Koppling av knappsatsläsare

Knappsatsläsare kopplas till en apparat på samma sätt som närhetsläsare.

Se: AN0006-SE - Så lägger man till en läsare <www.paxton.info/6132>

# Konfiguration av läsarens driftsläge

1. Navigera till den enhet som har en läsare knuten till sig
2. I fliken "**Konfiguration**", tryck på "**Visa mer**" vid "**Läsare**"
3. Markera rutan bredvid "Autentiseringsalternativ" för att aktivera val av driftsläge
4. Välj önskat driftsläge

För åtkomstpunkter kan in- och utpasseringsläsare ha olika driftslägen (t ex kräva passerbricka + PIN för att få åtkomst till byggnaden, men endast kräva passerbricka för att få lämna den).

5. Om Bluetooth-baserade autentiseringsmetoder (smarta enheter eller Paxton10:s handsfree-passerbricka) används, välj läsräckvidden för dessa metoder och markera "**Verifiering**" om användare av smarta enheter måste konfigurera PIN eller biometrik på sin enhet för att de ska vara giltiga.

Se: AN0006-SE- Så lägger man till läsare <www.paxton.info/6132> för mer information om Bluetooth-baserade autentiseringsmetoder.

Om ett annat driftsläge krävs för en viss tid går det att använda "**Tidsbaserad autentisering**".

6. Slutför stegen ovan för "**Autentiseringsalternativ**"
7. Markera rutan bredvid "Tidsbaserad autentisering" för att aktivera ytterligare driftslägen
8. Klicka på "**Välj**" och välj den tidsprofil som krävs för olika driftslägen
9. Konfigurera läsarens driftsläge, Bluetooth-läge och verifieringsinställningar som ska gälla för vald tidsprofil

(T ex kan autentiseringsalternativen definieras som "**passerbricka + kod**", medan det under arbetstid, när det alltid finns personer i byggnaden, är mer praktiskt att använda alternativet "**passerbricka**" eller "**kod**")

Om inga autentiseringsalternativ markerats kommer läsarna ha driftsläget "**endast passerbricka**".

# Förvaltning av koder

Koder förvaltas per enhet och kan användas av vilken användare som helst.

När en kods driftsläge har angetts, klicka på "**Förvalta koder**" i enhetens "**Läsare**" för att skapa en kod för den. Ange en kod, klicka på "**Lägg till**" eller välj en befintlig kod och klicka på "**Ta bort**" för att ta bort den.

Varje enhet kan ha flera koder.

# Förvaltning av PIN-koder

PIN-koder är unika för varje användare och behandlas som autentiseringsuppgift i användarposter.

För att ge användare en PIN-uppgift:

1. Öppna användarens uppgifter och klicka på fliken "**Uppgifter**"
2. Klicka på "**Lägg till uppgift**"
3. Välj "**PIN**" från rullistan
4. Ange en ny PIN-kod eller godkänn den slumpmässigt genererade
5. Klicka på "**OK**"

PIN-kodens längd kan ändras i systemalternativen.

# Vanliga frågor

Vad är skillnaden mellan PIN-kod och kod?

På engelska står "PIN" för "**Personal Identification Number**" (personligt identifieringsnummer) och är unikt för varje användare. Alla användare har sin egen PIN som endast ger åtkomst till enheter som de har byggnadsbehörighet till.

I jämförelse anges kod på varje enhet och kan användas av flera användare. Det går inte att använda kod för att identifiera användare, varför de inte begränsas av byggnadsbehörigheter.

Hur långa är PIN-koder?

PIN-koden måste vara mellan 4 och 8 siffror långa. Detta konfigureras i systemalternativ. Alla PIN-koder i ett visst system måste vara lika långa.

Mina unika PIN-koder har tagit slut. Vad ska jag göra?

PIN-kodens längd kan ändras i systemalternativ. Genom att öka PIN-kodens längd kommer antalet PIN-kombinationer att öka, vilket även ökar systemsäkerheten.

OBS: Om systemets PIN-längd ökar leder det till att nollor läggs till i slutet av alla befintliga PIN-koder så att det nya längdkravet uppfylls.

Varning! Om systemets PIN-längd minskar tas alla PIN-autentiseringsuppgifter bort.

Hur långa är koder?

Koder måste vara mellan 4 och 8 siffror långa. Koder kan ha olika längd.

Varför kan en viss enhet ha flera olika koder?

Det finns flera scenarion där en viss enhet kan ha flera koder, t ex:

- En kod till parkeringsbommen som ges till besökare och som byts varje vecka. Den kod som används av anställda är dock konstant.

- Olika koder motsvarar olika åtkomstnivåer, t ex där högre chefer använder en viss kod som fungerar på alla enheter, medan t ex städare använder en annan kod som endast fungerar på vissa enheter.

Påverkar ett kodbaserat driftsläge anti-passback eller närvarotagning?

När driftsläget "Endast kod" används är användaren okänd - därför kan inte positionen bestämmas. För närvarotagning och anti-passback-begränsning krävs ett driftsläge som består av en autentiseringsmetod (passerbricka eller PIN).